

1 IAP20 Rec'd PCT/PTO 23 JUN 2006

## 明細書

## 被認証装置及び認証装置及び認証方法

## 5 技術分野

本発明は、被認証装置、或いは認証装置に関する。または、上記認証装置と上記被認証装置との間で認証をおこなう認証方法に関する。

## 背景技術

10 利用者があるサービスを受けるとき、サービスを受けられる正当な利用者であるかどうか本人確認（認証）が行なわれ、暗号通信のための鍵共有が行なわれる。暗号通信に用いられる暗号アルゴリズムは1種類であり、異なるアルゴリズムを実装している装置間では認証及び鍵共有が行えない。

15 また、複数の暗号技術利用プロトコルの利用が可能な通信システムについての記載が載った文献が存在する（特開平10-304333号公報）。

また、複数のアルゴリズムを用いた技術についての記載が載った文献が存在する（特開2000-151578号公報，特開平5-2271  
20 52号公報）。

以上のように、従来は、暗号通信に用いられる暗号アルゴリズムは1種類であるため、アルゴリズムの脆弱性が発見されたり、解読されたり、鍵の漏洩等によりデータ暗号化によるセキュリティ（安全）が保たれ  
25 なくなった場合に、より安全なアルゴリズム等を実装することになるが、これにより装置間で異なるアルゴリズムを実装する場合が生じ、上述したように異なるアルゴリズムを実装している装置間では認証及び鍵共

有が行えないといった問題があった。また、各メーカー等がそれぞれ販売等している暗号アルゴリズムがあるために、異なるアルゴリズムを実装している装置間では認証及び鍵共有が行なえないといった問題があった。

5       また、上述したようにセキュリティ（安全）が保たれなくなった場合に、より安全なアルゴリズムを実装することになるが、新たなアルゴリズム等を実装することによりそれまでのシステム及び装置が使い物にならなくなるといった問題があった。

10       また、将来、より高度なアルゴリズムが考案されたとしてもそれまで使用していた装置に適用することができないといった問題があった。

本発明は、搭載しているアルゴリズムが異なるために認証が行なえないといった問題を解決することを目的とする。

本発明は、1つのアルゴリズムが解読等により使用できなくなっても引き続きシステム及び装置を運用可能とすることを目的とする。

15       また、本発明は、引き続きシステム及び装置を運用可能とすることで、アルゴリズムの解読等によるセキュリティ低下というリスクを軽減することを目的とする。

また、本発明は、盗聴等による不正な解読等の機会を減らし、セキュリティを向上させることを目的とする。

20

## 発明の開示

この発明に係る被認証装置は、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する記憶部と、

25       上記記憶部により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信する送信部と、

上記認証装置から上記送信部により送信された少なくとも1つのアル

ゴリズム識別子と少なくとも1つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部と、

5 上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子に基づいて上記認証装置との間で認証処理をおこなう認証処理部と  
を備えたことを特徴とする。

また、上記記憶部は、1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶し、

10 上記送信部は、上記記憶部により1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信し、

15 上記受信部は、上記認証装置から上記送信部により送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から所定のプロファイルとして組となる上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とを受信し、

20 上記認証処理部は、上記受信部により受信された所定のプロファイルとして組となる所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする。

また、上記記憶部は、さらに、記憶された少なくとも1つのアルゴリズム識別子に対応する少なくとも1つのアルゴリズムを1つのセットとした上記セットを示すバージョンを識別するバージョン識別子を記憶し、

25 上記送信部は、上記記憶部により記憶されたバージョン識別子を認証

装置に送信し、

上記受信部は、上記認証装置から上記送信部により送信されたバージョン識別子が識別するバージョンが示すセットとなる少なくとも1つのアルゴリズムの中の所定のアルゴリズムに対応する上記所定のアルゴリ

5      ズム識別子を受信し、

上記認証処理部は、上記受信部により受信された所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする。

10      また、この発明に係る認証装置は、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する記憶部と、

被認証装置から少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを受信する受信部と、

上記受信部により受信された少なくとも1つのアルゴリズム識別子と  
15      少なくとも1つの暗号鍵識別子との中に上記記憶部により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とが存在する場合に、上記受信部により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から上記記憶部により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを  
20      選択する選択部と、

上記選択部により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記被認証装置に送信する送信部と、

上記送信部により送信される所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなう認証  
25      処理部と

を備えたことを特徴とする。

また、上記記憶部は、少なくとも1つのアルゴリズム識別子の1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子の1つの暗号鍵識別子とを組とする少なくとも1つのプロファイルを識別する少なくとも1つのプロファイル識別子を記憶し、

- 5      上記受信部は、さらに、上記被認証装置から少なくとも1つのプロファイル識別子を受信し、

- 上記選択部は、上記受信部により受信された少なくとも1つのプロファイル識別子の中に上記記憶部により記憶された少なくとも1つのプロファイル識別子が存在する場合に、上記受信部により受信された少なくとも1つのプロファイル識別子の中から上記記憶部により記憶される所定のプロファイル識別子を選択し、
- 10

    上記送信部は、上記選択部により選択された所定のプロファイル識別子を上記被認証装置に送信し、

- 上記認証処理部は、上記送信部により送信される所定のプロファイル識別子により識別される所定のプロファイルが組とする上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなうことを特徴とする。
- 15

- また、上記記憶部は、さらに、記憶された少なくとも1つのアルゴリズム識別子に対応する少なくとも1つのアルゴリズムを1つのセットとして、上記セットのバージョンを識別するバージョン識別子を記憶し、
- 20

    上記受信部は、さらに、上記被認証装置から所定のバージョン識別子を受信し、

- 上記選択部は、上記受信部により受信された所定のバージョン識別子が識別するバージョンが示すセットの中の1つのアルゴリズムに対応する上記所定のアルゴリズム識別子を選択し、
- 25

    上記送信部は、上記選択部により選択された所定のアルゴリズム識別

子を上記被認証装置に送信し、

上記認証処理部は、上記送信部により送信される所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなうことを特徴とする。

この発明に係る認証方法は、複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信する第1の送信工程と、

少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する認証装置が、上記第1の送信工程により被認証装置から送信された複数のアルゴリズム識別子と複数の暗号鍵識別子とを受信する第1の受信工程と、

上記第1の受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とが存在する場合に、上記認証装置が上記受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第2の送信工程と、

上記被認証装置が上記認証装置から上記第2の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第2の受信工程と、

上記第2の受信工程により受信された所定のアルゴリズム識別子と所

定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で  
認証処理をおこなう認証処理工程とを備えたことを特徴とする。

また、この発明に係る認証方法は、少なくとも1つのアルゴリズム識  
別子と少なくとも1つの暗号鍵識別子とを記憶する被認証装置から記憶  
5 された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵  
識別子とを認証装置に送信する第1の送信工程と、

複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する認証装  
置が、上記第1の送信工程により被認証装置から送信された少なくとも  
1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを受信す  
10 る第1の受信工程と、

上記第1の受信工程により受信された少なくとも1つのアルゴリズム  
識別子と少なくとも1つの暗号鍵識別子との中に上記認証装置により記  
憶された複数のアルゴリズム識別子の少なくとも1つと複数の暗号鍵識  
別子の少なくとも1つとが存在する場合に、上記認証装置が上記受信工  
15 程により受信された少なくとも1つのアルゴリズム識別子と少なくとも  
1つの暗号鍵識別子との中から上記認証装置により記憶される所定のア  
ルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗  
号鍵識別子とを上記認証装置から上記被認証装置に送信する第2の送信  
20 工程と、

上記被認証装置が上記認証装置から上記第2の送信工程により送信さ  
れた所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第2  
の受信工程と、

上記第2の受信工程により受信された所定のアルゴリズム識別子と所  
25 定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で  
認証処理をおこなう認証処理工程とを備えたことを特徴とする。

# 図面の簡単な説明

図 1 は、実施の形態 1 における認証システムの構成を示す図である。

5 図 2 は、実施の形態 1 における認証方法を示すフローチャート図である。

図 3 は、通信情報 1 のフレームの一例を示す図である。

図 4 は、通信情報 2 のフレームの一例を示す図である。

図 5 は、通信情報 3 のフレームの一例を示す図である。

図 6 は、通信情報 4 のフレームの一例を示す図である。

10 図 7 は、通信装置 200 側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムと個別鍵とを示す図である。

図 8 は、通信装置 100 側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムとを示す図である。

図 9 は、実施の形態 2 における認証システムの構成を示す図である。

15 図 10 は、実施の形態 2 における認証方法を示すフローチャート図である。

図 11 は、実施の形態 3 における認証方法を示すフローチャート図である。

20 図 12 は、実施の形態 4 における認証方法を示すフローチャート図である。

図 13 は、実施の形態 5 における認証方法を示すフローチャート図である。

図 14 は、ハードウェア構成図である。

25 発明を実施するための最良の形態  
実施の形態 1.



図 1 は、実施の形態 1 における認証システムの構成を示す図である。

図 1 において、認証システムは、認証装置となる通信装置 100 と被  
認証装置となる通信装置 200 とを備えている。通信装置 100 は、ア  
ンテナ 101、通信処理部 110、記憶部 120、制御部 130、選択  
5 部 160、認証処理部 196 を備えている。通信処理部 110 は、受信  
部 111、送信部 112 を有している。認証処理部 196 は、暗号処理  
部 140、乱数生成部 150、個別鍵生成部 170、一時鍵生成部 18  
0、認証用データ 1 生成部 190、認証用データ 2 チェック部 195 を  
有している。通信装置 200 は、アンテナ 201、通信処理部 210、  
10 記憶部 220、制御部 230、認証処理部 296 を備えている。通信処  
理部 210 は、受信部 211、送信部 212 を有している。認証処理部  
296 は、暗号処理部 240、乱数生成部 250、一時鍵生成部 280  
、認証用データ 1 チェック部 290、認証用データ 2 生成部 295 を有  
している。実施の形態 1 では、通信装置 100 と通信装置 200 とは、  
15 アンテナ 101、201 を介して無線通信する場合を説明するが、これ  
に限るものではなく有線通信であっても構わない。例えば、ETC（料  
金自動収集）、ドライブスルー等において、通信装置 100 は、店舗側  
の路側機として、通信装置 200 は、自動車側の車載機として構成され  
る。

20 図 2 は、実施の形態 1 における認証方法を示すフローチャート図であ  
る。

記憶部 120 は、少なくとも 1 つのアルゴリズム識別子と少なくとも  
1 つの暗号鍵識別子と、上記少なくとも 1 つのアルゴリズム識別子の各  
アルゴリズム識別子に対応するアルゴリズムを記憶している。また、上  
25 記記憶部 120 は、少なくとも 1 つのアルゴリズム識別子の 1 つのアル  
ゴリズム識別子と少なくとも 1 つの暗号鍵識別子の 1 つの暗号鍵識別子

とを組とする少なくとも1つのプロファイルを識別する少なくとも1つのプロファイル識別子を記憶している。

記憶部220は、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子と、上記少なくとも1つのアルゴリズム識別子の各  
5 アルゴリズム識別子に対応するアルゴリズムと上記少なくとも1つの暗号鍵識別子の各暗号鍵識別子に対応する暗号鍵となる装置固有の個別鍵と装置固有番号とを記憶している。また、上記記憶部220は、1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とプロファイルを識別する少なくとも1つのプロファイル識別子とを記憶している。  
10

ここで、通信装置100、200のうち、少なくとも一方において、アルゴリズム識別子と暗号鍵識別子との組が複数存在すればよい。

S（ステップ）201において、認証処理工程の一部として、乱数生成部150は、乱数1を生成する。  
15

S202において、送信工程として、送信部112は、乱数生成部150により生成された乱数1を通信情報1として通信装置200に送信する。例えば、通信装置200を搭載した自動車が、通信装置100により図示していない検知器により検知された場合に、送信部112は、  
20 乱数1を通信装置200に送信する。通信装置100は、乱数1を通信情報1として通信装置200に送信することで、通信装置200が保持している鍵情報（鍵識別子、アルゴリズム識別子）を要求する。言い換えれば、通信情報1が通信装置200への要求情報となる。

S203において、受信工程として、受信部211は、送信部112により送信された乱数1を通信情報1として受信する。通信装置200では、受信部211が、乱数1を受信したことにより、通信装置100  
25

より通信装置 200 が保持している鍵情報（鍵識別子、アルゴリズム識別子）が要求されたと判断する。

S 204 において、認証処理工程の一部として、乱数生成部 250 は、乱数 2 を生成する。

- 5        S 205 において、送信工程（第 1 の送信工程）として、送信部 212 は、上記記憶部 220 により記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子と装置固有番号と、乱数生成部 250 により生成された乱数 2 とを通信情報 2 として認証装置である通信装置 200 に送信する。ここで、1 つのアルゴリズム識別子と 1 つ
- 10        の暗号鍵識別子とを 1 組みとしてプロファイルとして表し、通信情報 2 は、乱数 2 と装置固有番号と組数分のプロファイル数とプロファイル数分の各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とをデータとして有している。さらに、ここでは、各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とを対応させたデータとしている。言い換えれば、上記送信部 212
- 15        は、上記記憶部 220 により 1 つのアルゴリズム識別子と 1 つの暗号鍵識別子とを 1 組のプロファイルとして記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを認証装置となる通信装置 100 に送信する。
- 20

- S 206 において、受信工程（第 1 の受信工程）として、受信部 111 は、被認証装置となる通信装置 200 から、乱数 2 と装置固有番号と組数分のプロファイル数とプロファイル数分の少なくとも 1 つのプロファイル識別子と少なくとも 1 つのプロファイル識別子の各プロファイル
- 25        識別子に対応した少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを有する通信情報 2 を受信する。

S 2 0 7において、選択工程として、選択部 1 6 0は、上記受信部 1 1 1により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中に上記記憶部 1 2 0により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とが存在する場合に、上記受信部 1 1 1により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から上記記憶部 1 2 0により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する。言い換えれば、上記選択部 1 6 0は、上記受信部 1 1 1により受信された少なくとも1つのプロファイル識別子の中に上記記憶部 1 2 0により記憶された少なくとも1つのプロファイル識別子が存在する場合に、上記受信部 1 1 1により受信された少なくとも1つのプロファイル識別子の中から上記記憶部 1 2 0により記憶される所定のプロファイル識別子を選択する。所定のプロファイル識別子を選択することで、所定のプロファイル識別子が示すプロファイルに組みする所定のアルゴリズム識別子と所定の暗号鍵識別子とが選択される。例えば、単純に、通信装置 1 0 0， 2 0 0双方が共通して有しているアルゴリズム識別子と暗号鍵識別子とを選択してもよいし、暗号解読等により既にセキュリティが十分でなくなったアルゴリズム識別子と暗号鍵識別子とを排除した上で、通信装置 1 0 0， 2 0 0双方が共通して有しているアルゴリズム識別子と暗号鍵識別子とを選択してもよい。また、実施の形態 1では、所定のプロファイル識別子を選択することで、所定のプロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とを選択する。

S 2 0 8において、認証処理工程の一部として、個別鍵生成部 1 7 0は、上記選択部 1 6 0により選択された所定の暗号鍵識別子に対応する暗号鍵となる通信装置 2 0 0が有している個別鍵を通信情報 2の装置固

有番号から例えばハッシュ値等を用いて生成する。

S 2 0 9において、認証処理工程の一部として、一時鍵生成部 1 8 0 は、上記選択部 1 6 0により選択された所定のアルゴリズム識別子に対応するアルゴリズムを用いて所定の暗号鍵識別子に対応する暗号鍵となる個別鍵生成部 1 7 0により生成された個別鍵で乱数 1, 2を暗号処理部 1 4 0を用いて暗号化し、認証処理用暗号鍵の一例となる一時鍵を生成する。

S 2 1 0において、認証処理工程の一部として、認証用データ 1 生成部 1 9 0は、乱数 2のすべて或いは一部を暗号処理部 1 4 0により一時鍵生成部 1 8 0により生成された一時鍵で暗号化することにより認証用データ 1を生成する。

S 2 1 1において、送信工程（第 2 の送信工程）として、送信部 1 1 2は、上記選択部 1 6 0により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子と上記選択部により選択された対応する所定のプロフィール識別子と認証用データ 1 生成部 1 9 0により生成された認証用データ 1とを通信情報 3として上記被認証装置となる通信装置 2 0 0に送信する。

S 2 1 2において、受信部 2 1 1は、上記認証装置となる通信装置 1 0 0から上記送信部 2 1 2により送信された少なくとも 1つのアルゴリズム識別子と少なくとも 1つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子と所定のアルゴリズム識別子と所定の暗号鍵識別子と対応するプロフィール識別子と認証用データ 1とを通信情報 3として受信する。言い換えれば、上記受信部 2 1 1は、上記認証装置となる通信装置 1 0 0から上記送信部 2 1 2により送信された少なくとも 1つのアルゴリズム識別子と少なくとも 1つの暗号鍵識別子との中から所定のプロフィールとして組となる所定のアルゴリズ

ム識別子と所定の暗号鍵識別子とを受信する。

5 S 2 1 3において、認証処理工程の一部として、暗号処理部 2 4 0 は、受信部 2 1 1 により受信されたプロファイル識別子を確認し、プロファイル識別子に対応する所定の暗号鍵識別子と所定のアルゴリズム識別子とを確認する。

10 S 2 1 4において、認証処理工程の一部として、一時鍵生成部 2 8 0 は、受信部 2 1 1 により受信され、暗号処理部 2 4 0 により確認された所定のアルゴリズム識別子に対応するアルゴリズムを用いて、記憶部 2 2 0 に記憶された個別鍵で乱数 1, 2 を暗号処理部 2 4 0 を用いて暗号化し、認証処理用暗号鍵の一例となる上記一時鍵を生成する。以上により通信装置 1 0 0, 2 0 0 間で同じ一時鍵という鍵共有ができたことになる。なお、記憶部 2 2 0 に記憶された個別鍵は、個別鍵生成部 1 7 0 と同様の生成方法で生成されたものであり、あらかじめ、I C カード等何かしらの手段を用いて記憶部 2 2 0 に記録されている。なお、この実  
15 施形態では、一時鍵生成部 1 8 0, 2 8 0 が一時鍵生成の際、個別鍵で暗号化したか、認証装置と被認証装置とが同じ処理を実施すればよいため、復号してもよい。

20 S 2 1 5において、認証処理工程の一部として、認証用データ 1 チェック部 2 9 0 は、受信部 2 1 1 により通信情報 3 として受信された暗号化されている認証用データ 1 を一時鍵生成部 2 8 0 により生成された一時鍵により暗号処理部 2 4 0 を用いて復号する。

25 S 2 1 6において、認証処理工程の一部として、認証用データ 1 チェック部 2 9 0 は、復号した認証用データ 1 のデータが、通信装置 2 0 0 が通信装置 1 0 0 に送信した乱数 2 のすべて或いは一部であるかどうかを確認する。復号した認証用データ 1 のデータが乱数 2 のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置 1 0 0 との間で

認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置 100, 200 間での認証処理の一方が成功したことを意味する。

5 S 2 1 7 において、認証処理工程の一部として、認証用データ 2 生成部 2 9 5 は、乱数 1 のすべて或いは一部を暗号処理部 2 4 0 により一時鍵生成部 2 8 0 により生成された一時鍵で暗号化することにより認証用データ 2 を生成する。

10 S 2 1 8 において、認証処理工程の一部の送信工程として、送信部 2 1 2 は、認証用データ 2 生成部 2 9 5 により生成された認証用データ 2 を通信情報 4 として通信装置 1 0 0 に送信する。

S 2 1 9 において、認証処理工程の一部の受信工程として、受信部 1 1 1 は、通信装置 2 0 0 から認証用データ 2 を通信情報 4 として受信する。

15 S 2 2 0 において、認証処理工程の一部として、認証用データ 2 チェック部 1 9 5 は、受信部 1 1 1 により通信情報 4 として受信された暗号化されている認証用データ 2 を一時鍵生成部 1 8 0 により生成された一時鍵により暗号処理部 1 4 0 を用いて復号する。

20 S 2 2 1 において、認証処理工程の一部として、認証用データ 2 チェック部 1 9 5 は、復号した認証用データ 2 のデータが、通信装置 1 0 0 が通信装置 2 0 0 に送信した乱数 1 のすべて或いは一部であるかどうかを確認する。復号した認証用データ 2 のデータが乱数 1 のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置 2 0 0 との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置 1 0 0, 2 0 0 間での認証処理の他方が成功したことを意味する。

25

以上により、通信装置 1 0 0, 2 0 0 間での認証処理が終了し、その

後は、通信装置 100, 200 間で一時鍵を用いて暗号化されたデータを通信することにより、データの安全性が確保される。

図 3 は、通信情報 1 のフレームの一例を示す図である。

図 3 において、通信情報 1 は、ヘッダと乱数 1 データを有している。

5 図 4 は、通信情報 2 のフレームの一例を示す図である。

図 4 において、通信情報 2 は、ヘッダと乱数 2 データと装置固有番号（装置固有 No.）とプロファイル数（Profile 数）と各プロファイルを識別するプロファイル識別子としての Profile 1, . . . Profile n と、各プロファイル識別子に対応するアルゴリズム識別子（アルゴリズム ID）と暗号鍵識別子（鍵 ID）とを有している。図 4 では、各プロファイル識別子と各プロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

図 5 は、通信情報 3 のフレームの一例を示す図である。

15 図 5 において、通信情報 3 は、ヘッダと選択された所定のプロファイルを識別する所定のプロファイル識別子としての Profile k と、所定のプロファイル識別子に対応するアルゴリズム識別子（アルゴリズム ID）と暗号鍵識別子（鍵 ID）と認証用データ 1 とを有している。図 5 では、所定のプロファイル識別子と所定のプロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

図 6 は、通信情報 4 のフレームの一例を示す図である。

図 6 において、通信情報 4 は、ヘッダと認証用データ 2 とを有している。

25 図 7 は、通信装置 200 側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムと個別鍵とを示す図である。



図 7 において、通信装置 200 側では、記憶部 220 に、プロフィール x x のアルゴリズム識別子 (ID) と暗号鍵識別子 (ID) とアルゴリズム識別子に対応するアルゴリズム x と暗号鍵識別子に対応する個別鍵 x と、プロフィール y y のアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズム y と暗号鍵識別子に対応する個別鍵 y と、・・・プロフィール z z のアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズム z と暗号鍵識別子に対応する個別鍵 z とが記憶されている。すなわち、通信装置 200 に搭載 (実装) されている。

図 8 は、通信装置 100 側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムとを示す図である。

図 8 において、通信装置 100 側では、記憶部 120 に、プロフィール a a のアルゴリズム識別子 (ID) と暗号鍵識別子 (ID) とアルゴリズム識別子に対応するアルゴリズム 1 と、プロフィール b b のアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズム 2 と、・・・プロフィール c c のアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズム n とが記憶されている。すなわち、通信装置 100 に搭載 (実装) されている。

以上のように、認証処理部 296 は、上記受信部 211 により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置となる通信装置 100 との間で認証処理をおこなう。すなわち、認証処理部 296 は、上記受信部 211 により受信された所定のアルゴリズム識別子に対応するアルゴリズムと上記受信部により受信された所定の暗号鍵識別子に対応する暗号鍵とを用いて認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記認証装置となる通信装置 100 との間で認証処理をおこなう。言い

換えれば、上記認証処理部296は、上記受信部211により受信された所定のプロファイルとして組となる所定のアルゴリズム識別子に対応するアルゴリズムと所定の暗号鍵識別子に対応する暗号鍵とを用いて上記認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記認証装置との間で認証処理をおこなう。

一方、認証処理部196は、上記送信部112により送信される所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記被認証装置となる通信装置200との間で認証処理をおこなう。すなわち、認証処理部196は、上記送信部112により送信される所定のアルゴリズム識別子に対応するアルゴリズムと上記送信部112により送信された所定の暗号鍵識別子に対応する暗号鍵とを用いて認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記被認証装置となる通信装置200との間で認証処理をおこなう。言い換えれば、上記認証処理部196は、上記送信部112により送信される所定のプロファイル識別子により識別される所定のプロファイルが組とする所定のアルゴリズム識別子に対応するアルゴリズムと所定の暗号鍵識別子に対応する暗号鍵とを用いて上記認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記被認証装置との間で認証処理をおこなう。

ここで、制御部130は、通信装置100の各部を制御する。また、制御部230は、通信装置200の各部を制御する。また、記憶部120は、通信装置100の各部で行なわれる処理中に生じるデータを記憶する。また、記憶部220は、通信装置200の各部で行なわれる処理中に生じるデータを記憶する。

例えば、一例として、ETC、ドライブスルー等において、通信装置100が、店舗側の路側機として、通信装置200が、自動車側の車載

機として構成される場合に、以上のステップを概括すると以下のようになる。

まず、店舗側の路側機は、車載機に対して、車載機が保持している鍵情報（鍵識別子、アルゴリズム識別子）を要求する。

- 5       そして、車載機は、自身が保持している鍵に関する全情報を路側機に送信する。

次に、路側機は、受け取った鍵情報の中から、自身が保持しているアルゴリズム識別子と鍵識別子とが一致しているものを選択し、車載機に選択したアルゴリズム識別子と鍵識別子とを知らせる。

- 10       以降、路側機及び車載機は、お互いに共通に保持していたアルゴリズム識別子と鍵識別子とに対応する共通鍵を用いて認証及び鍵共有を実施する。

- 15       以上のように、本実施の形態 1 は、暗号通信に用いるアルゴリズムを複数に対応させるもので、1つのアルゴリズムが解読等で使用できなくなっても他のアルゴリズムを使用することで、引き続きシステムを運用可能とし、アルゴリズム解読等によるセキュリティ低下というリスクを軽減させることができる。また、複数のアルゴリズムを使いこなすことにより、同一のアルゴリズムを使用する回数が減ることにより、不正の攻撃者による解読の機会を減らし、セキュリティを向上させることができる。
- 20       さらに、新たに考案されたアルゴリズムを通信装置に搭載することができることから、新たに考案されたアルゴリズムの適用をも容易にすることができる。通信装置 100, 200のうち、少なくとも一方において、アルゴリズム識別子と鍵識別子との組が複数存在すれば、選択肢ができることになり、上記効果が得られる。なお、この実施形態 1 で
- 25       は、装置 100, 200の少なくとも一方に複数のアルゴリズム識別子と暗号鍵識別子との組が複数存在すればよいとした。しかし、この発明

はアルゴリズム識別子と暗号鍵識別子の少なくとも1組が一致すれば認証が行えるため、必ずしも装置100, 200の少なくとも一方に複数組存在する必要はなく各装置に1組だけが存在していてもよい。また、各装置に1組だけしか存在していてもよいことから、一つの暗号アルゴリズムしか使用しない従来例にもこの発明による認証方法を適用可能である。

## 実施の形態2.

図9は、実施の形態2における認証システムの構成を示す図である。

図9において、通信装置200における認証処理部296は、図1の構成に対し、さらに、認証用データ1生成部291を有している。その他の各構成は、図1と同様である。

図10は、実施の形態2における認証方法を示すフローチャート図である。

図10において、図2のS215, S216がS1015, S1016に代わった以外は、図2と同様である。

S1015において、認証処理工程の一部として、認証用データ1生成部291は、乱数2のすべて或いは一部を暗号処理部240により一時鍵生成部280により生成された一時鍵で暗号化することにより認証用データ1を生成する。

S1016において、認証処理工程の一部として、認証用データ1チェック部290は、通信情報3として受信部211により受信された暗号化されたままの認証用データ1と認証用データ1生成部291により生成された認証用データ1とが一致するかどうかを確認する。一致すれば、不正の攻撃者との間ではなく、通信装置100との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、

通信装置 1 0 0, 2 0 0 間での認証処理の一方が成功したことを意味する。

以上のように構成しても実施の形態 1 と同様の効果を得ることができる。

5

実施の形態 3.

実施の形態 3 における各構成は、図 1 と同様である。

図 1 1 は、実施の形態 3 における認証方法を示すフローチャート図である。

10 図 1 1 では、図 2 の S 2 0 2, S 2 0 3 が無いこと以外は、図 2 と同様である。

実施の形態 3 では、認証側となる通信装置 1 0 0 が通信装置 2 0 0 に通信情報 1 を送信しなくても通信装置 2 0 0 から通信装置 1 0 0 へ通信情報 2 を送信する構成となっている。かかるステップを省略することにより、より高速に認証フローを実施することができる。

15

以上のように構成しても実施の形態 1 と同様の効果を得ることができる。

実施の形態 4.

20 実施の形態 4 における各構成は、図 1 と同様である。

図 1 2 は、実施の形態 4 における認証方法を示すフローチャート図である。

図 1 2 では、図 2 の S 2 0 5, S 2 0 6, S 2 0 7, S 2 1 1, S 2 1 2 が、S 1 2 0 5, S 1 2 0 6, S 1 2 0 7, S 1 2 1 1, S 1 2 1 2 に代わった以外は、図 2 と同様である。

25

実施の形態 4 では、記憶部 2 2 0 は、さらに、記憶された少なくとも

1つのアルゴリズム識別子に対応する少なくとも1つのアルゴリズムを1つのセットとした上記セットを示すバージョンを識別するバージョン識別子（ID）を記憶する。

5 同様に、記憶部120は、さらに、記憶された少なくとも1つのアルゴリズム識別子に対応する少なくとも1つのアルゴリズムを1つのセットとして、上記セットのバージョンを識別するバージョン識別子（ID）を記憶する。

例えば、バージョン識別子としてのバージョン1が識別するバージョンは、アルゴリズムとしてDESだけをサポートする。バージョン2が  
10 識別するバージョンは、アルゴリズムとしてDES、MISTYをサポートする。バージョン3が識別するバージョンは、アルゴリズムとしてDES、MISTY、Camellia、AESをサポートする。

S1205において、送信工程（第1の送信工程）として、送信部212は、上記記憶部220により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子と装置固有番号と、乱数生成部250により生成された乱数2と、さらに、記憶部220により記憶されたバージョン識別子とを通信情報2-1として認証装置である通信装置100に送信する。

S1206において、受信工程（第1の受信工程）として、受信部111は、被認証装置となる通信装置200から、乱数2と装置固有番号と組数分のプロファイル数とプロファイル数分の少なくとも1つのプロファイル識別子と少なくとも1つのプロファイル識別子の各プロファイル識別子に対応した少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子と、さらに、所定のバージョン識別子とを有する通信情報2-1を受信する。  
25

S1207において、選択工程として、選択部160は、上記受信部

1 1 1により受信された所定のバージョン識別子が識別するバージョン  
 が示すセットの中に上記記憶部 1 2 0により記憶された少なくとも1つ  
 のアルゴリズムが存在する場合に、上記受信部 1 1 1により受信された  
 所定のバージョン識別子が識別するバージョンが示すセットの中から上  
 5 記記憶部 1 2 0により記憶されるアルゴリズムに対応する所定のアルゴ  
 リズム識別子を選択する。例えば、通信装置 2 0 0が古いバージョンし  
 か対応していない場合に、古いバージョンが示すアルゴリズムがすべて  
 セキュリティ上問題がある場合、選択せずに以降の認証処理を終了させ  
 ることもできる。一方、1つでも認証処理に使用可能なアルゴリズムが  
 10 あれば、その使用可能なアルゴリズムを使って、以降の認証処理を行な  
 わせることができる。バージョン識別子を用いることで、バージョン識  
 別子から通信装置 2 0 0が使用可能なアルゴリズムを搭載しているかど  
 うかを判断することができる。

S 1 2 1 1において、送信工程（第2の送信工程）として、送信部 1  
 15 1 2は、上記選択部 1 6 0により選択された所定のアルゴリズム識別子  
 と認証用データ 1 生成部 1 9 0により生成された認証用データ 1 とを通  
 信情報 3 - 1として上記被認証装置となる通信装置 2 0 0に送信する。

S 1 2 1 2において、受信工程として、受信部 2 1 1は、上記認証装  
 置となる通信装置 1 0 0から上記送信部 2 1 2により送信されたバージ  
 20 ョン識別子が識別するバージョンが示すセットとなる上記記憶部 2 2 0  
 により記憶された少なくとも1つのアルゴリズムの中から選択された所  
 定のアルゴリズムに対応する所定のアルゴリズム識別子と認証用データ  
 1 とを通信情報 3 - 1として受信する。

以降、認証処理部 2 9 6は、上記受信部 2 1 1により受信された所定  
 25 のアルゴリズム識別子に対応する所定のアルゴリズムと上記所定のアル  
 ゴリズム識別子と組となる所定の暗号鍵識別子に対応する所定の暗号鍵

とを用いて上記認証処理用暗号鍵を生成し、生成された認証処理用暗号鍵を用いて上記認証装置との間で認証処理をおこなう。

- 5 同様に、認証処理部 1 9 6 は、上記送信部 1 1 2 により送信される所定のアルゴリズム識別子に対応するアルゴリズムと上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子に対応する暗号鍵とを用いて上記認証処理用暗号鍵を生成し、生成された認証処理用暗号鍵を用いて上記被認証装置との間で認証処理をおこなう。

以上のように構成することで、実施の形態 1 の効果に加え、セキュリティ上問題がある古いバージョンを排除することもできる。

- 10 ここで、実施の形態 4 では、選択部 1 6 0 が、所定のアルゴリズム識別子を選択しているが、さらに、選択した所定のアルゴリズム識別子に対応する所定の暗号鍵識別子を選択してもかまわない。かかる場合、図 1 2 における S 1 2 1 1, S 1 2 1 2 は、図 2 における S 2 1 1, S 2 1 2 のままで構わない。

15

実施の形態 5.

実施の形態 5 における各構成は、図 1 と同様である。

図 1 3 は、実施の形態 5 における認証方法を示すフローチャート図である。

- 20 図 1 3 では、図 2 の S 2 0 5、S 2 0 6、S 2 0 7 が、S 1 3 0 5、S 1 3 0 6、S 1 3 0 7、S 1 3 0 8、S 1 3 0 9、S 1 3 1 0、S 1 3 1 1、S 1 3 0 7 に代わった以外は、図 2 と同様である。

- 25 実施の形態 5 では、実施の形態 4 と同様に、記憶部 2 2 0 は、さらに、記憶された少なくとも 1 つのアルゴリズム識別子に対応する少なくとも 1 つのアルゴリズムを 1 つのセットとした上記セットを示すバージョンを識別するバージョン識別子 (ID) を記憶する。



同様に、記憶部 1 2 0 は、さらに、記憶された少なくとも 1 つのアルゴリズム識別子に対応する少なくとも 1 つのアルゴリズムを 1 つのセットとして、上記セットのバージョンを識別するバージョン識別子 (ID) を記憶する。

5        S 1 3 0 5 において、送信工程として、送信部 2 1 2 は、上記記憶部 2 2 0 により記憶された装置固有番号と、乱数生成部 2 5 0 により生成された乱数 2 と、さらに、記憶部 2 2 0 により記憶されたバージョン識別子とを通信情報 2 - 2 として認証装置である通信装置 2 0 0 に送信する。

10       S 1 3 0 6 において、受信工程 (第 1 の受信工程) として、受信部 1 1 1 は、被認証装置となる通信装置 2 0 0 から、乱数 2 と装置固有番号と所定のバージョン識別子とを有する通信情報 2 - 2 を受信する。

      S 1 3 0 7 において、選択工程として、選択部 1 6 0 は、上記受信部 1 1 1 により受信された所定のバージョン識別子が、記憶部 1 2 0 に記憶されたバージョン識別子と一致する場合は、そのバージョン識別子を選択し、一致しない場合には、所定のバージョン識別子が示すセットの中に上記記憶部 1 2 0 により記憶された少なくとも 1 つのアルゴリズムが存在する場合に、上記記憶部 1 2 0 により記憶された少なくとも 1 つのアルゴリズムが存在するセットを示すバージョンのバージョン識別子  
15        を選択する。例えば、記憶部 1 2 0 に記憶されたバージョン識別子の方が、上記受信部 1 1 1 により受信された所定のバージョン識別子より最新バージョンのバージョン識別子である場合に、通信装置 1 0 0, 2 0 0 に共通するように古いバージョンとなる上記受信部 1 1 1 により受信された所定のバージョン識別子を選択する。通信装置 1 0 0, 2 0 0 に  
20        共通する古いバージョンを選択することにより以降の認証処理を続行させ、鍵共有をおこなうことができる。

S 1 3 0 8において、送信工程として、送信部 1 1 2 は、選択部 1 6 0により選択されたバージョン識別子（I D）を通信情報 2－3として通信装置 2 0 0に送信する。

5 S 1 3 0 9において、受信工程として、受信部 2 1 1 は、通信装置 1 0 0よりバージョン識別子（I D）を通信情報 2－3として受信する。

S 1 3 1 0において、送信工程として、送信部 2 1.2 は、上記記憶部 2 2 0により記憶された少なくとも1つのプロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子と組数分のプロファイル数とを通信情報 2－4として認証  
10 装置である通信装置 2 0 0に送信する。

S 1 3 1 1において、受信工程として、受信部 1 1 1 は、被認証装置となる通信装置 2 0 0から、少なくとも1つのプロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子と組数分のプロファイル数とを通信情報 2－4として  
15 受信する。ここで、乱数 2と装置固有番号とを通信情報 2－2に含めているが、通信情報 2－4に含めていても構わない。

S 1 3 1 2において、選択工程として、選択部 1 6 0は、上記受信部 1 1 1により受信された少なくとも1つのプロファイル識別子の中に上記記憶部 1 2 0により記憶された少なくとも1つのプロファイル識別子が存在する場合に、上記受信部 1 1 1により受信された少なくとも1つのプロファイル識別子の中から上記記憶部 1 2 0により記憶される所定の  
20 プロファイル識別子を選択する。所定のプロファイル識別子を選択することで、所定のプロファイル識別子が示すプロファイルに組みする所定のアルゴリズム識別子と所定の暗号鍵識別子とが選択される。

25 以上のように、実施の形態 5では、実施の形態 4と比較し、まず、バージョン選択という工程を別に行なう形態である。以上のように構成し

ても実施の形態 4 と同様の効果を得ることができる。そして、実施の形態 1 の効果に加え、セキュリティ上問題があるアルゴリズムを排除することもできる。

5 以上のように、上記実施の形態における認証方法は、複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信する第 1 の送信工程と、少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを記憶する認証装置が、上記第 1 の送信工程により被認証装置から送信された複数のアルゴリズム識別子と複数の暗  
10 号鍵識別子とを受信する第 1 の受信工程と、上記第 1 の受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とが存在する場合に、上記認証装置が上記受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、上記選択工程により  
15 選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第 2 の送信工程と、上記被認証装置が上記認証装置から上記第 2 の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第 2 の受信工程と、  
20 上記第 2 の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えている。

25 或いは、少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを記憶する被認証装置から記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを認証装置に送信

する第 1 の送信工程と、複数のアルゴリズム識別子と複数の暗号鍵識別  
 子とを記憶する認証装置が、上記第 1 の送信工程により被認証装置から  
 送信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗  
 号鍵識別子とを受信する第 1 の受信工程と、上記第 1 の受信工程により  
 5 受信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗  
 号鍵識別子との中に上記認証装置により記憶された複数のアルゴリズム  
 識別子の少なくとも 1 つと複数の暗号鍵識別子の少なくとも 1 つとが存  
 在する場合に、上記認証装置が上記受信工程により受信された少なくと  
 も 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中か  
 10 ら上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗  
 号鍵識別子とを選択する選択工程と、上記選択工程により選択された所  
 定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上  
 記被認証装置に送信する第 2 の送信工程と、上記被認証装置が上記認証  
 装置から上記第 2 の送信工程により送信された所定のアルゴリズム識別  
 15 子と所定の暗号鍵識別子とを受信する第 2 の受信工程と、上記第 2 の受  
 信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別  
 子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこ  
 なう認証処理工程とを備えている。

以上の説明において、各実施の形態の説明において「～部」として説  
 20 明したものは、一部或いはすべてコンピュータで動作可能なプログラム  
 により構成することができる。これらのプログラムは、例えば、C 言語  
 により作成することができる。或いは、HTML や SGML や XML を  
 用いても構わない。

図 1 4 は、ハードウェア構成図である。

25 以上の説明において、各実施の形態の説明において「～部」として説  
 明したものを、一部或いはすべてコンピュータで動作可能なプログラム

により構成する場合、図14に示すように、通信装置100、200は、プログラムを実行するCPU (Central Processing Unit) 37を備えている。CPU37は、内蔵された、或いはバス38を介してRAM (Random Access Memory) 40 (記憶装置、記憶部の一例である)、外部と通信可能な通信ポート44に接続されている。また、図14に示すように、ROM (Read Only Memory) 39、磁気ディスク装置46等の記憶装置に接続されていても構わない。

プログラムにより構成する場合、図14におけるプログラム群49には、各実施の形態の説明において「～部」として説明したものにより実行されるプログラムが記憶されている。プログラム群49は、上記記憶装置に記憶されている。プログラム群49は、CPU37、OS47等により実行される。記憶装置は、各処理の結果を記憶する。

また、各実施の形態の説明において「～部」として説明したものは、ROM39に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェア或いは、ハードウェア或いは、ソフトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。

また、上記各実施の形態を実施させるプログラムは、FD (Flexible Disk)、光ディスク、CD (コンパクトディスク)、MD (ミニディスク)、DVD (Digital Versatile Disk) 等のその他の記録媒体による記録装置を用いて記憶されても構わない。係る場合には、図14に示すように、FDD (Flexible Disk Drive) 45、コンパクトディスク装置 (CDD) 86等を備える。

25

産業上の利用可能性

このような通信装置 100, 200 は、ETC、ドライブスルー等における店舗側の路側機と自動車側の車載機に限らず、携帯電話等の移動体通信装置間、有線の通信装置間、或いは基地局を経由した有線と無線の通信装置間等における認証装置、被認証装置として、使用することができる。

本発明によれば、異なるアルゴリズムを実装している装置間でも認証及び鍵共有が行なえるようにすることができ、1つのアルゴリズムが解読等により使用できなくなっても引き続きシステム及び装置を運用可能とすることができる。

また、アルゴリズムの解読等によるセキュリティ低下というリスクを軽減することができる。

また、盗聴等による不正な解読等の機会を減らし、セキュリティを向上させることができる。

## 請求の範囲

1. 少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する記憶部と、

5      上記記憶部により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信する送信部と、

    上記認証装置から上記送信部により送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部と

10      、

    上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子に基づいて上記認証装置との間で認証処理をおこなう認証処理部と

    を備えたことを特徴とする被認証装置。

15      2. 上記記憶部は、1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶し、

    上記送信部は、上記記憶部により1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信し、

20      上記受信部は、上記認証装置から上記送信部により送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から所定のプロファイルとして組となる上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とを受信し、

25      上記認証処理部は、上記受信部により受信された所定のプロファイル

として組となる所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする請求項 1 記載の被認証装置。

5 3. 上記記憶部は、さらに、記憶された少なくとも 1 つのアルゴリズム識別子に対応する少なくとも 1 つのアルゴリズムを 1 つのセットとした上記セットを示すバージョンを識別するバージョン識別子を記憶し、

上記送信部は、上記記憶部により記憶されたバージョン識別子を認証装置に送信し、

10 上記受信部は、上記認証装置から上記送信部により送信されたバージョン識別子が識別するバージョンが示すセットとなる少なくとも 1 つのアルゴリズムの中の所定のアルゴリズムに対応する上記所定のアルゴリズム識別子を受信し、

15 上記認証処理部は、上記受信部により受信された所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする請求項 2 記載の被認証装置。

4. 少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを記憶する記憶部と、

20 被認証装置から少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを受信する受信部と、

上記受信部により受信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中に上記記憶部により記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とが存在する場合に、上記受信部により受信された少なくとも 1 つのアル  
25 ゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中から上記記憶部



により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択部と、

上記選択部により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記被認証装置に送信する送信部と、

- 5      上記送信部により送信される所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなう認証処理部と

を備えたことを特徴とする認証装置。

5.    上記記憶部は、少なくとも1つのアルゴリズム識別子の1つの
- 10    アルゴリズム識別子と少なくとも1つの暗号鍵識別子の1つの暗号鍵識別子とを組とする少なくとも1つのプロファイルを識別する少なくとも1つのプロファイル識別子を記憶し、

上記受信部は、さらに、上記被認証装置から少なくとも1つのプロファイル識別子を受信し、

- 15    上記選択部は、上記受信部により受信された少なくとも1つのプロファイル識別子の中に上記記憶部により記憶された少なくとも1つのプロファイル識別子が存在する場合に、上記受信部により受信された少なくとも1つのプロファイル識別子の中から上記記憶部により記憶される所定のプロファイル識別子を選択し、

- 20    上記送信部は、上記選択部により選択された所定のプロファイル識別子を上記被認証装置に送信し、

上記認証処理部は、上記送信部により送信される所定のプロファイル識別子により識別される所定のプロファイルが組とする上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とに基づいて上記被認証装置

- 25    との間で認証処理をおこなうことを特徴とする請求項4記載の認証装置。

6. 上記記憶部は、さらに、記憶された少なくとも1つのアルゴリズム識別子に対応する少なくとも1つのアルゴリズムを1つのセットとして、上記セットのバージョンを識別するバージョン識別子を記憶し、

5 上記受信部は、さらに、上記被認証装置から所定のバージョン識別子を受信し、

上記選択部は、上記受信部により受信された所定のバージョン識別子が識別するバージョンが示すセットの中の1つのアルゴリズムに対応する上記所定のアルゴリズム識別子を選択し、

10 上記送信部は、上記選択部により選択された所定のアルゴリズム識別子を上記被認証装置に送信し、

上記認証処理部は、上記送信部により送信される所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなうことを特徴とする請求項5記載の認証装置。

15 7. 複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信する第1の送信工程と、

20 少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する認証装置が、上記第1の送信工程により被認証装置から送信された複数のアルゴリズム識別子と複数の暗号鍵識別子とを受信する第1の受信工程と、

25 上記第1の受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とが存在する場合に、上記認証装置が上記受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子の中から上記認証装置により記憶さ

れる所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第2の送信工程と、

上記被認証装置が上記認証装置から上記第2の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第2の受信工程と、

上記第2の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えたことを特徴とする認証方法。

8. 少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する被認証装置から記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信する第1の送信工程と、

複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する認証装置が、上記第1の送信工程により被認証装置から送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを受信する第1の受信工程と、

上記第1の受信工程により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中に上記認証装置により記憶された複数のアルゴリズム識別子の少なくとも1つと複数の暗号鍵識別子の少なくとも1つとが存在する場合に、上記認証装置が上記受信工程により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から上記認証装置により記憶される所定のアル

ルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第2の送信工程と、

- 5      上記被認証装置が上記認証装置から上記第2の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第2の受信工程と、

- 10      上記第2の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えたことを特徴とする認証方法。

9. 複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信し、

- 15      少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する認証装置が、被認証装置から送信された複数のアルゴリズム識別子と複数の暗号鍵識別子とを受信し、

- 20      受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とが存在する場合に、上記認証装置が受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択し、

- 25      選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信し、

上記被認証装置が上記認証装置から送信された所定のアルゴリズム識

別子と所定の暗号鍵識別子とを受信し、

受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなうことを特徴とする認証方法。

- 5           10. 少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する被認証装置から記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信し、

- 10           複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する認証装置が、被認証装置から送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを受信し、

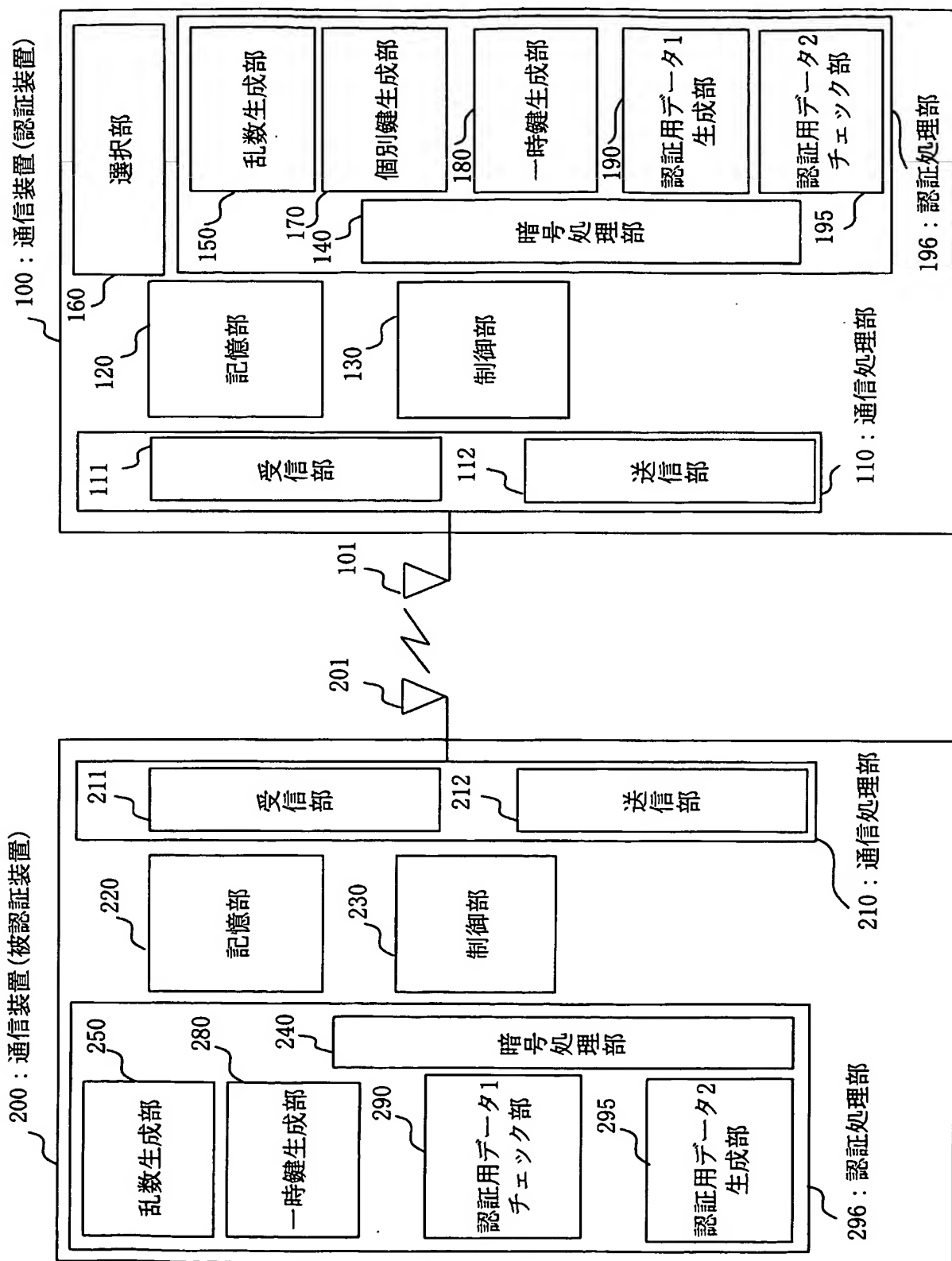
- 15           受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中に上記認証装置により記憶された複数のアルゴリズム識別子の少なくとも1つと複数の暗号鍵識別子の少なくとも1つとが存在する場合に、上記認証装置が受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択し、

- 20           選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信し、

上記被認証装置が上記認証装置から送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信し、

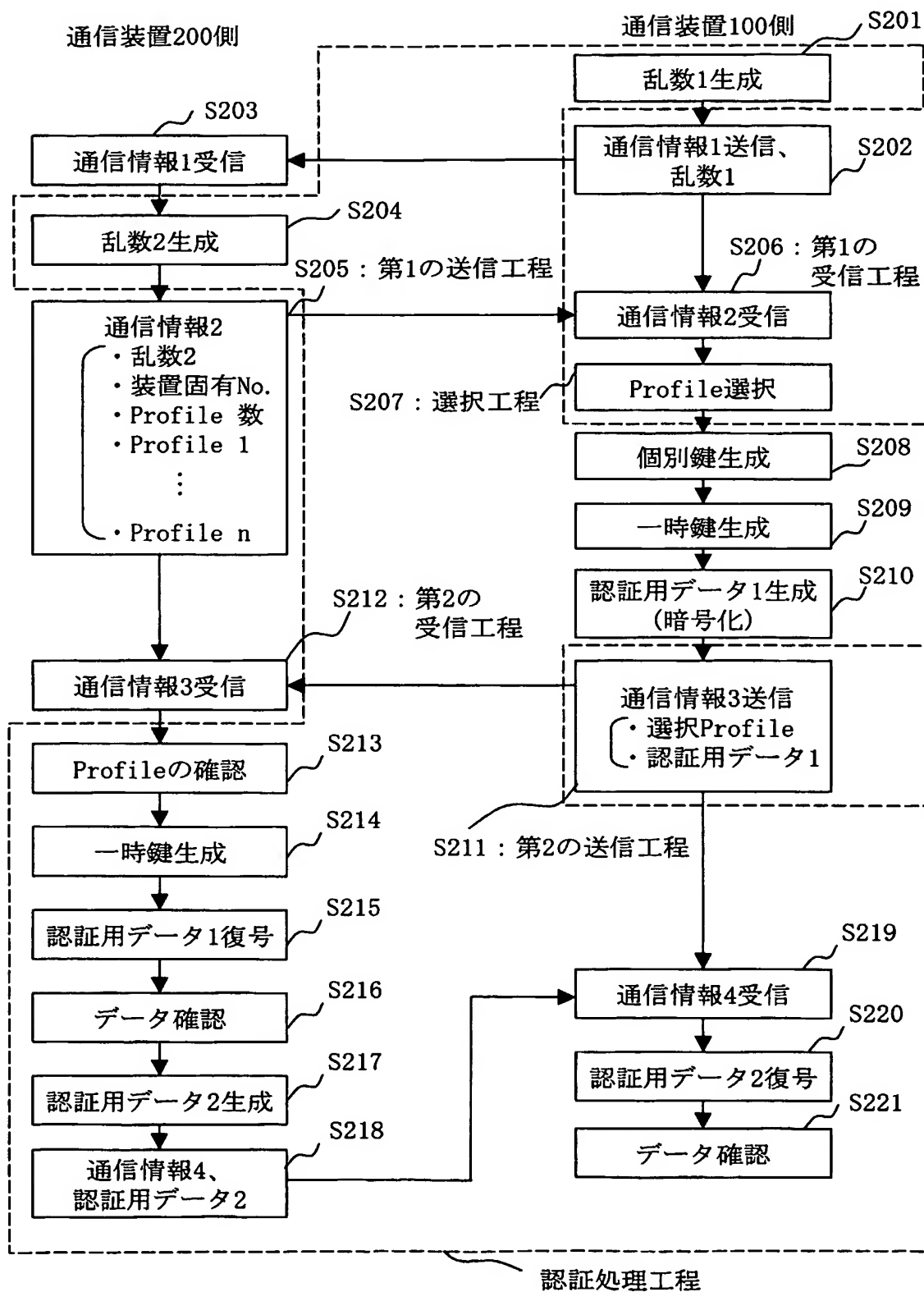
- 25           受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなうことを特徴とする認証方法。

図1



2/11

図2



3/11

図3

通信情報1

ヘッダ
乱数1

図4

通信情報2

ヘッダ		
乱数2		
装置固有No.		
Profile 数		
Profile 1	アルゴリズムID	鍵ID
.	.	.
.	.	.
.	.	.
Profile n	アルゴリズムID	鍵ID

図5

通信情報3

ヘッダ		
Profile k	アルゴリズムID	鍵ID
認証用データ1		



4/11

図6

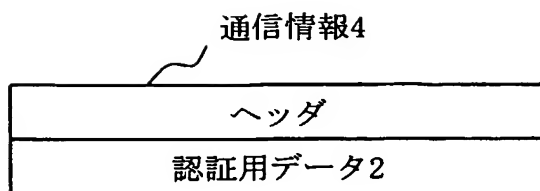


図7

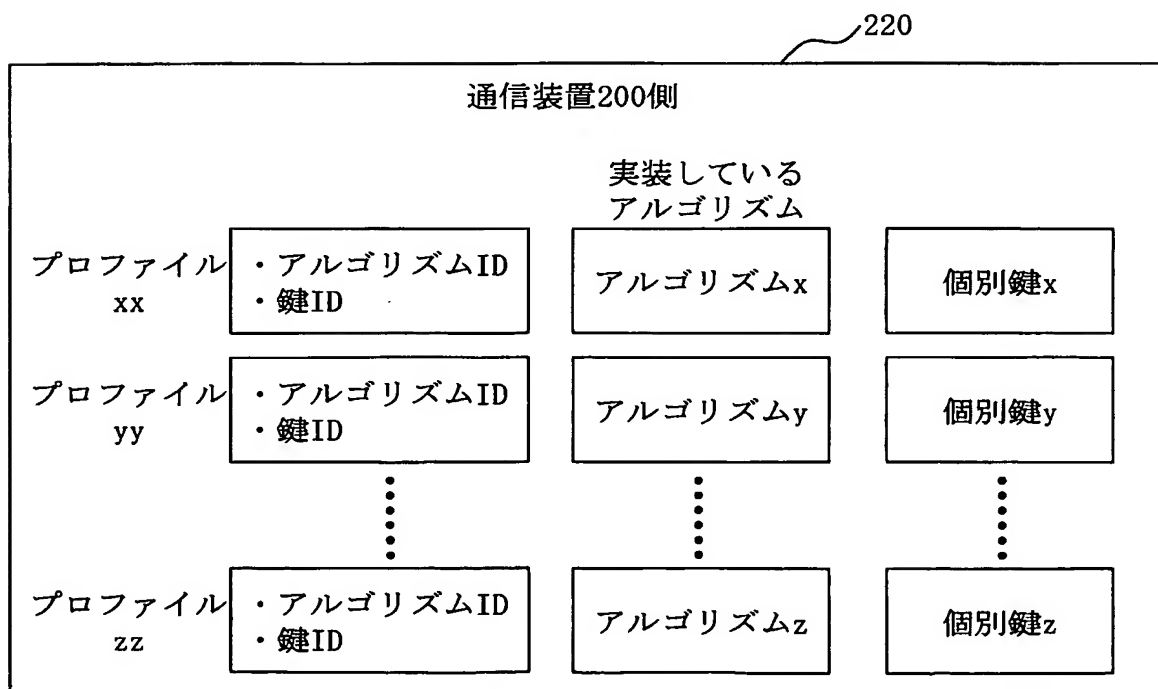


図8

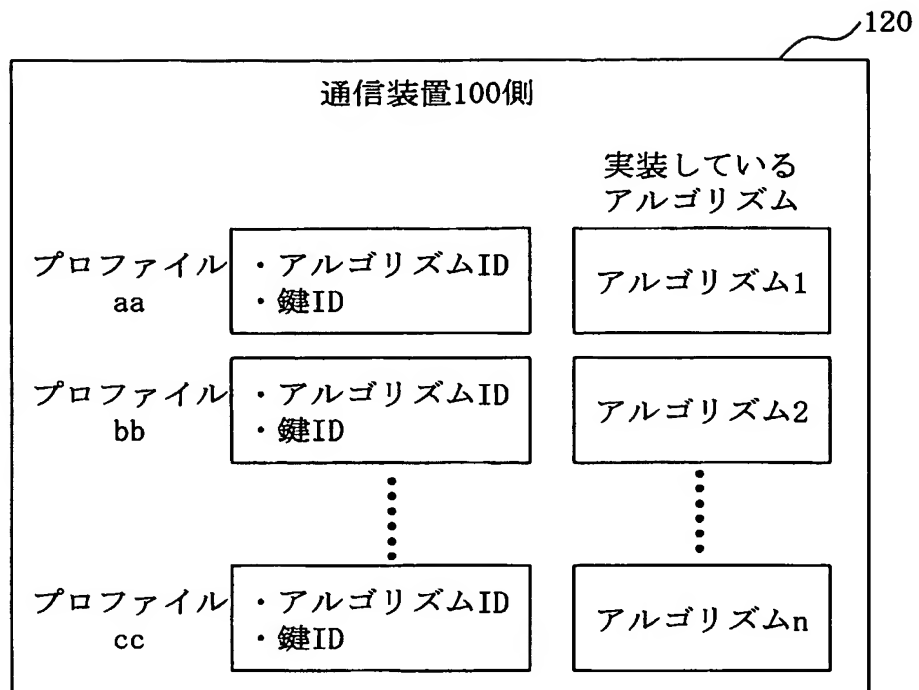
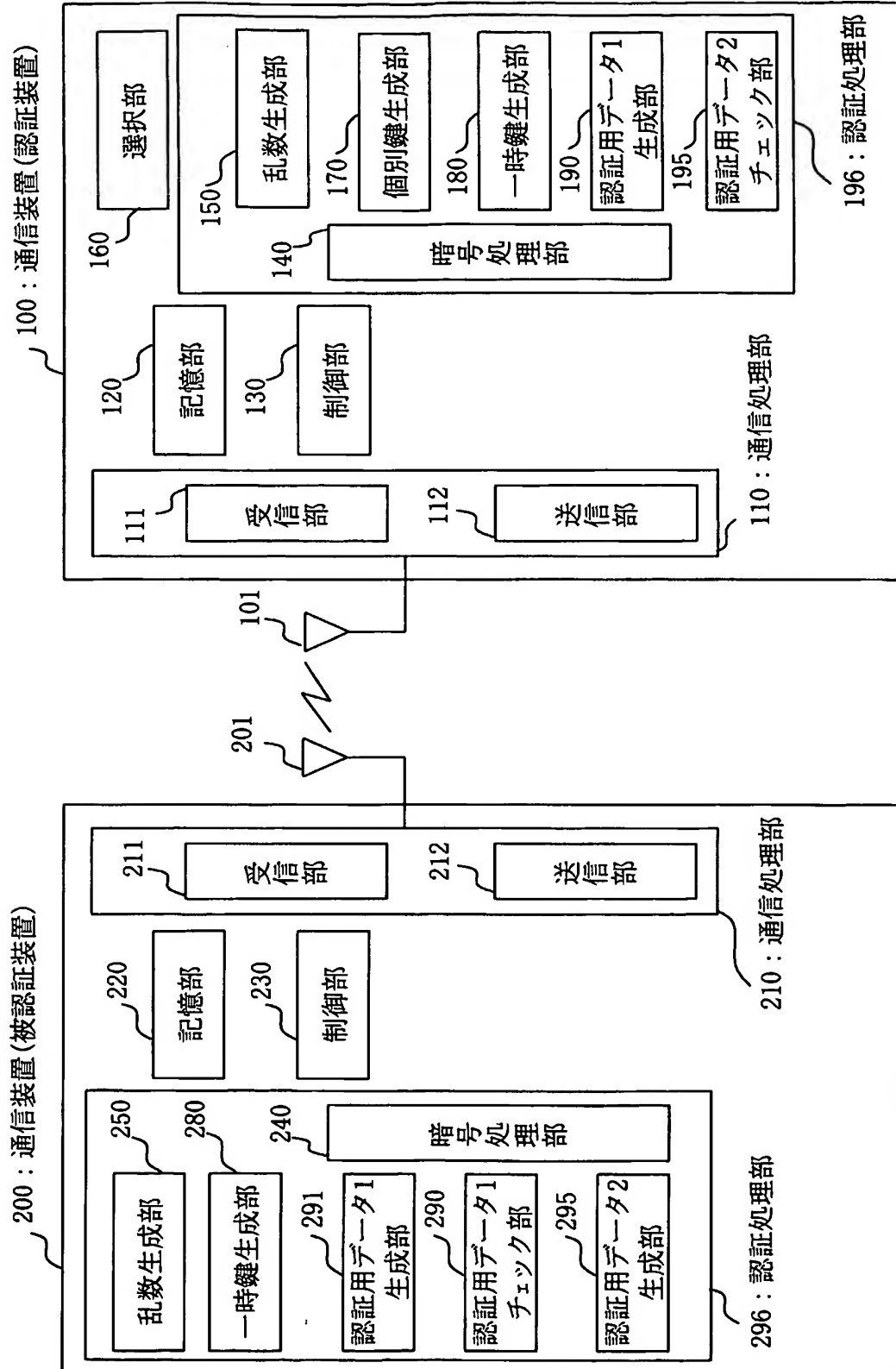
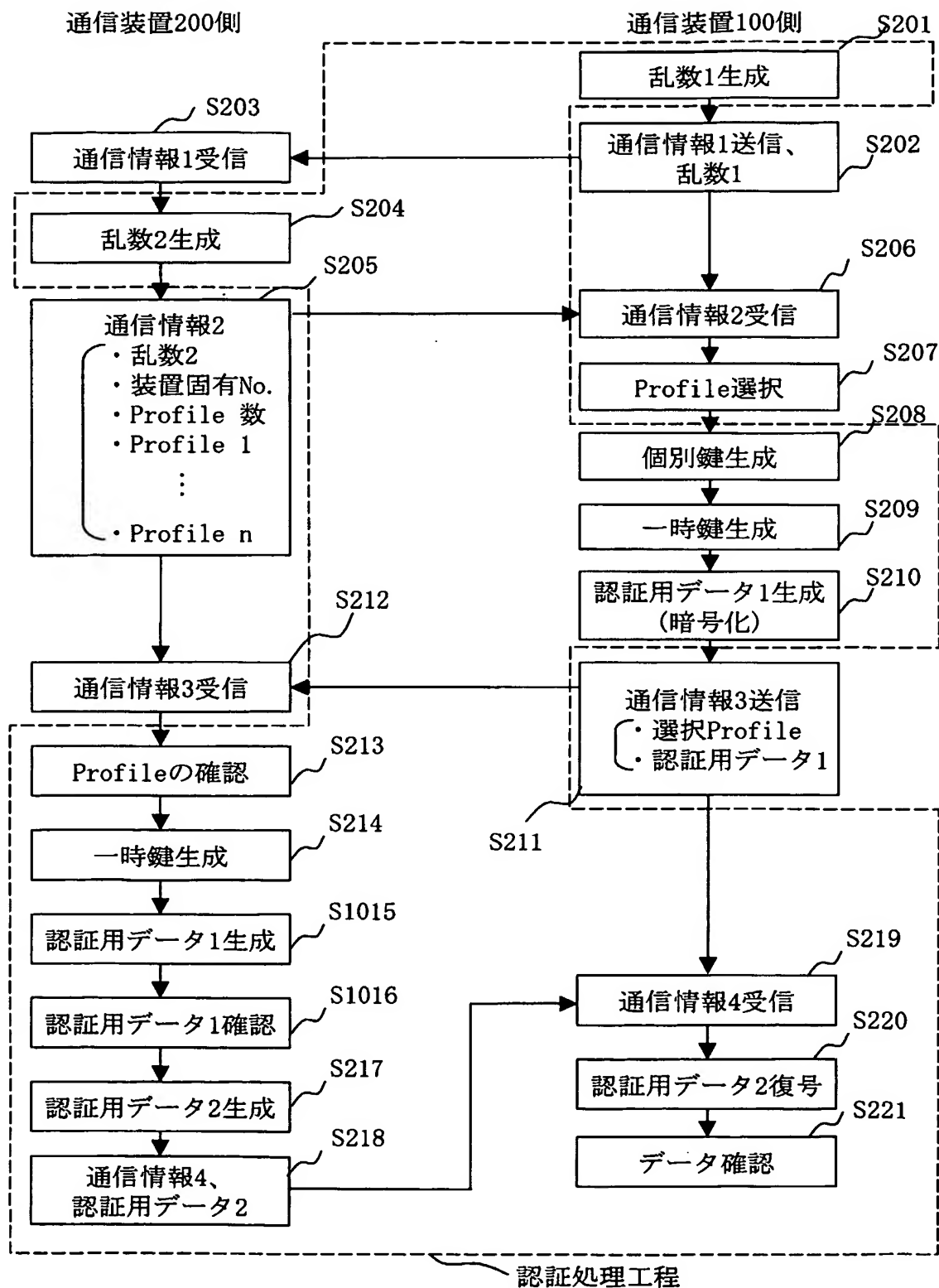


図9



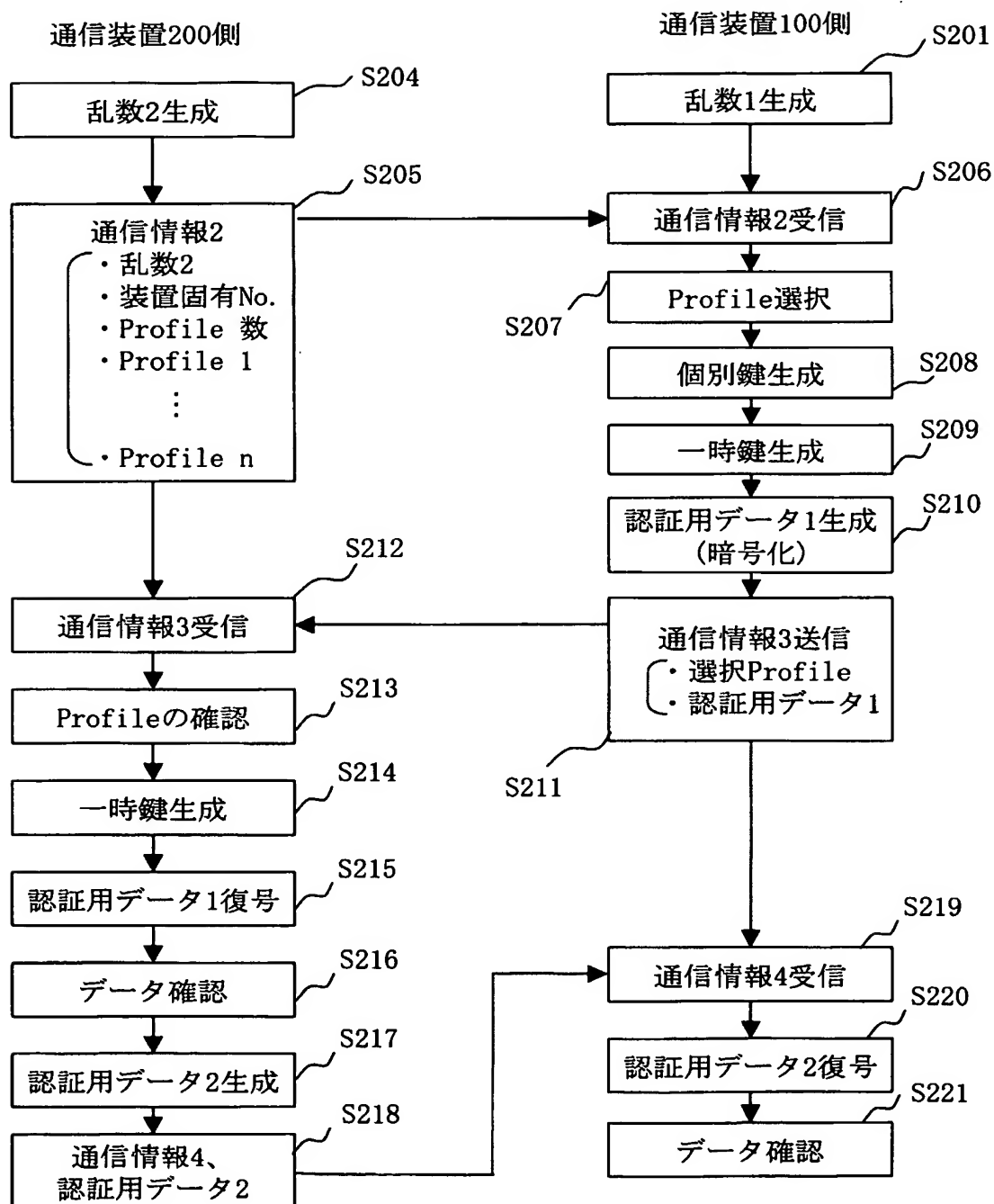
7/11

図10



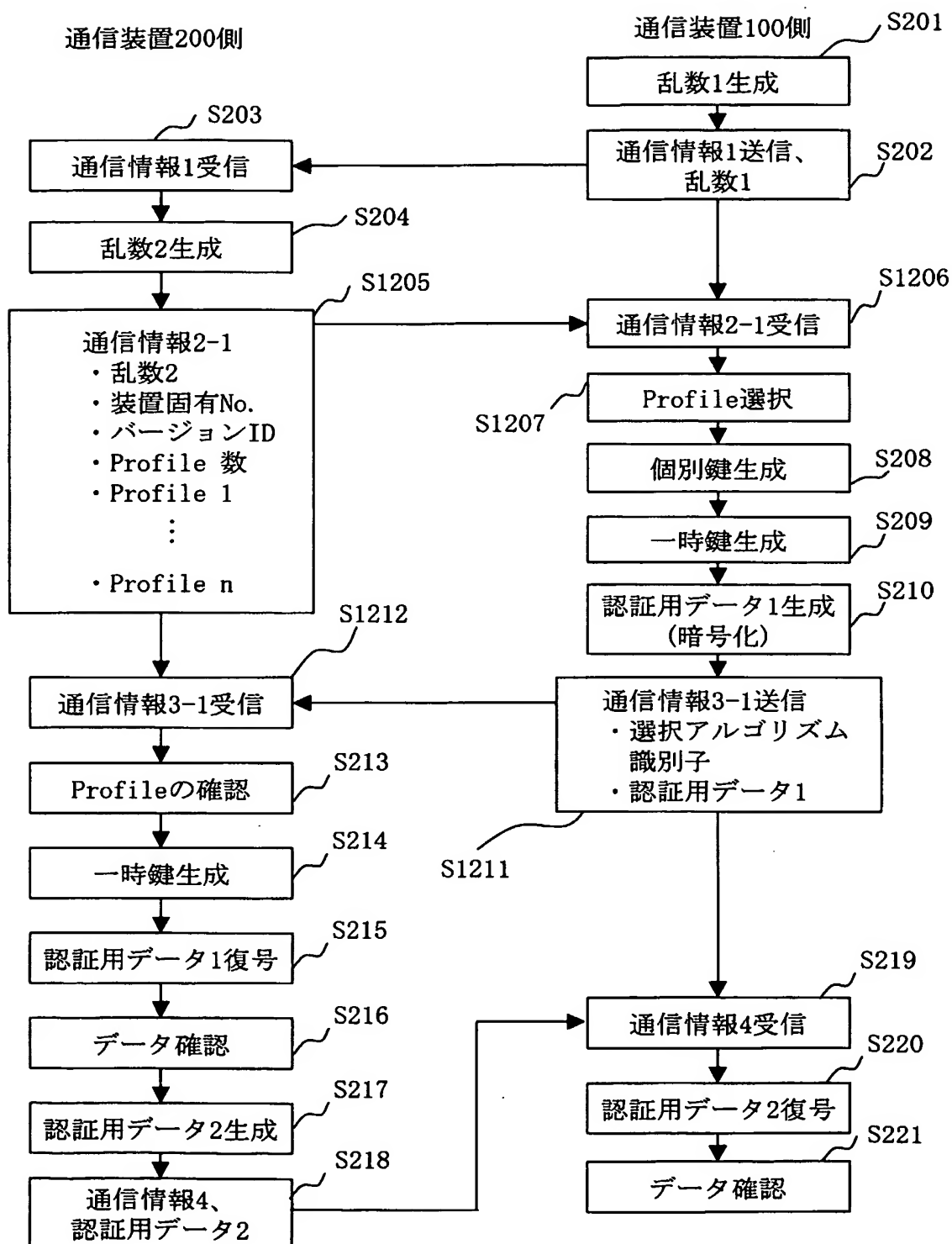
8/11

図11



9/11

図12



10/11

図13

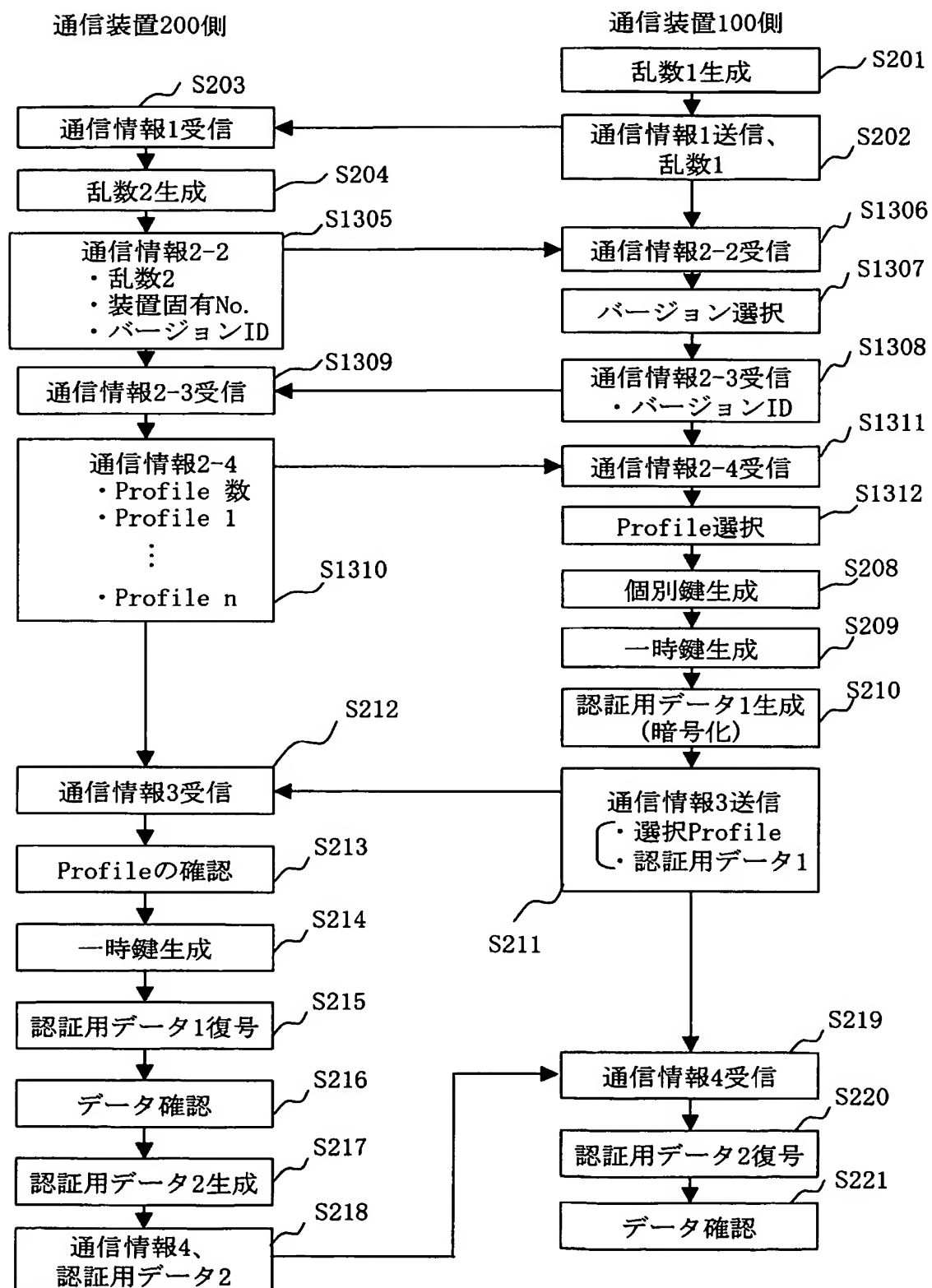
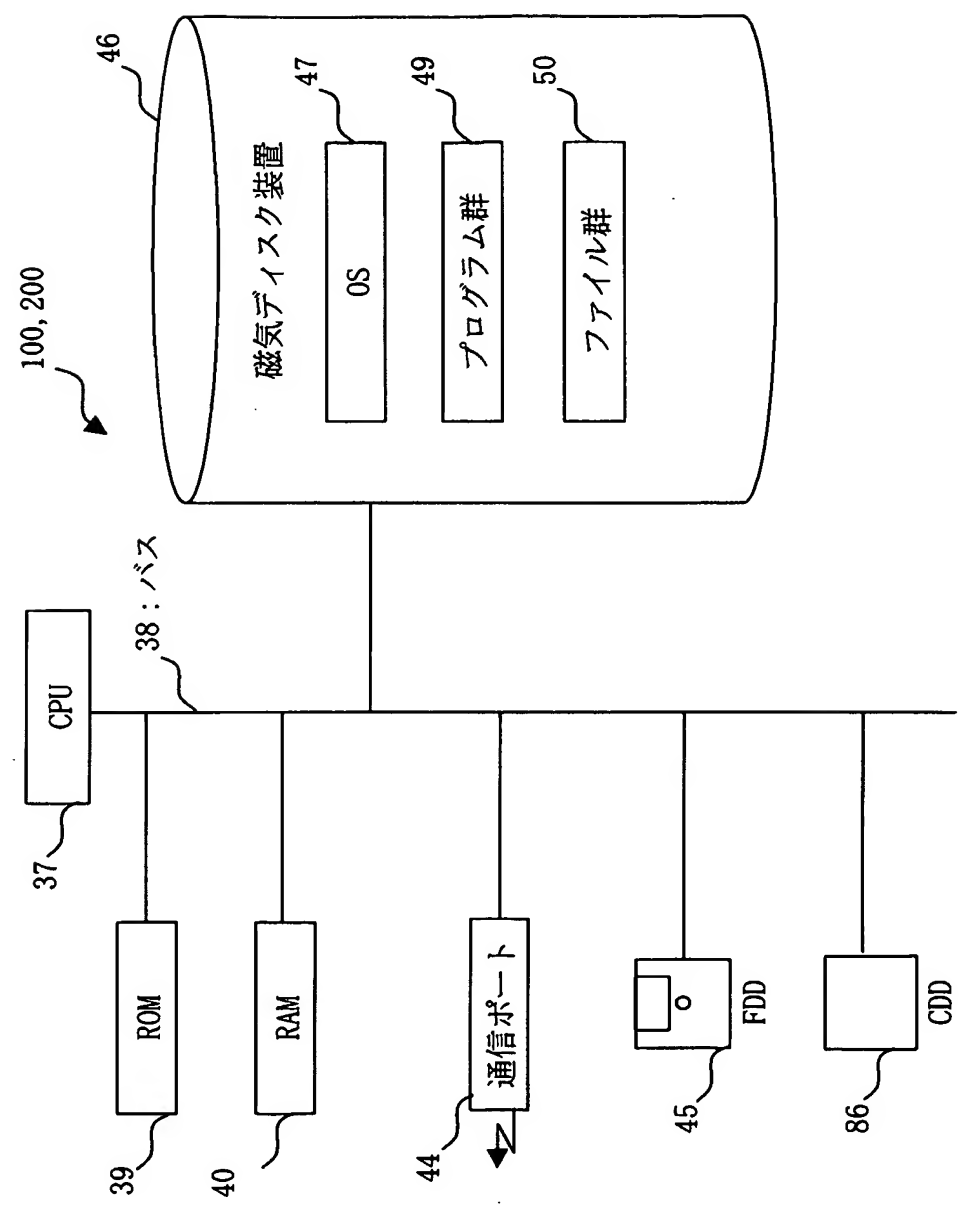


図14





## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/005881.

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L9/14, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04L9/14, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004

Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-274999 A (Hitachi, Ltd.), 08 October, 1999 (08.10.99), Figs. 5, 6 (Family: none)	1-10
Y	JP 2003-198530 A (Mitsubishi Electric Corp.), 11 July, 2003 (11.07.03), Figs. 9, 10 (Family: none)	1-10
Y	JP 9-83509 A (Hitachi, Ltd.), 28 March, 1997 (28.03.97), Figs. 4, 5 (Family: none)	1-10

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

## \* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
22 July, 2004 (22.07.04)

Date of mailing of the international search report  
10 August, 2004 (10.08.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/005881

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-293717 A (Matsushita Electric Industrial Co., Ltd.), 20 October, 2000 (20.10.00), Fig. 1 & EP 1043693 A	1-10
A	JP 2000-151578 A (Mitsubishi Electric Corp.), 30 May, 2000 (30.05.00), Full text (Family: none)	1-10
A	JP 2000-261427 A (Toshiba Corp.), 22 September, 2000 (22.09.00), Full text & EP 1035684 A	1-10
A	JP 11-328460 A (Mitsubishi Heavy Industries, Ltd.), 30 November, 1999 (30.11.99), Full text (Family: none)	1-10
A	JP 11-339080 A (Mitsubishi Heavy Industries, Ltd.), 10 December, 1999 (10.12.99), Full text (Family: none)	1-10

<b>A. 発明の属する分野の分類 (国際特許分類 (IPC))</b> Int. Cl <sup>7</sup> H04L 9/14, H04L 9/32		
<b>B. 調査を行った分野</b> 調査を行った最小限資料 (国際特許分類 (IPC)) Int. Cl <sup>7</sup> H04L 9/14, H04L 9/32		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2004年 日本国登録実用新案公報 1994-2004年 日本国実用新案登録公報 1996-2004年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
<b>C. 関連すると認められる文献</b>		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 11-274999 A (株式会社日立製作所) 1999. 10. 08, 第5, 6図 (ファミリーなし)	1-10
Y	JP 2003-198530 A (三菱電機株式会社) 2003. 07. 11, 第9, 10図 (ファミリーなし)	1-10
Y	JP 9-83509 A (株式会社日立製作所) 1997. 03. 28, 第4, 5図 (ファミリーなし)	1-10
<input checked="" type="checkbox"/> C欄の続きにも文献が列举されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願 の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 22. 07. 2004	国際調査報告の発送日 10. 8. 2004	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 石田 信行 5M 9469 電話番号 03-3581-1101 内線 3598	

様式PCT/ISA/210 (第2ページの続き) (2004年1月)

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record.**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**